Getting HIPAA Certified The EHNAC Way

Billy Jackson, Jr.
GSEC
Practical 1.4b

Overview

HIPAA- Health Insurance Portability and Accountability Act was enacted in 1996. Since then, there have been too many persons and organizations scrambling to try to interpret exactly what it all means. Mountains of published writings and hundreds of newly formed consulting companies have appeared and still the difficult task of determining what the legislation actually means to each person and corporation can be as clear as mud. Legislation that was intended to help protect the Civil rights of Americans has set the Healthcare Information Technology sector on its ear. Even in an environment of seasoned IT professionals, and within the EDI arena, confusion abounds. In a company that holds large amounts of PHI (Protected Healthcare Information), the fear is, how can we be as sure as possible that we are on track with what the legislation is trying to say and not be accused of being negligent with this PHI.

The title of this document is even cloudy. HIPAA certified? Is there such a creature? Well, that can even be debated in some circles. So what can we do? Out of the dust comes an organization especially made for this situation.

EHNAC:
(ELECTRONIC HEALTHCARE NETWORK ACCREDITATION COMMISSION

> EHNAC Accreditation provides independent peer evaluation of an organization's ability to perform at industry-established levels. EHNAC's process permits a review of current performance levels and, if necessary, helps to bring performance up to industry-established levels with assistance from the accrediting body and industry mentors. (EHNAC website, Default Page)

> EHNAC Healthcare Network Accreditation indicates that a VAN, clearinghouse, or other organization has met or exceeded EHNAC's performance criteria for EDI - a combination of speed, accuracy, and data integrity. EHNAC Accreditation is based on independent peer evaluation of an entity’s ability to perform at levels based on industry-established criteria. The accrediting process permits applicants to review their existing performance levels and to bring those levels into accordance with industry-established minimums and the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-91). (EHNAC website, Frequently Asked Questions for the Electronic Healthcare Transaction Industry)

The purpose of this document is to describe the process of obtaining a "Full Accreditation" from EHNAC. Of course this report will be written from a Security prospective. Some aspects of the procedures for going through the Accreditation process will be described. The security related areas will be described more fully while at most glossing over any area that might not have a security, privacy, or confidentiality concentration.

Introduction

It is the goal of a corporation to acquire what is called a Full Accreditation with EHNAC. This is done through a number of different actions taken by the company seeking the accreditation. These actions will usually be through various disclosures within a self-assessment report, supporting evidence, and much documentation. These assessments will be done in several areas relating to a company network for one. These are: Data Security/Privacy and Confidentiality, Technical Performance, Business Practices, and lastly Resources. The following briefly describes each one of these four areas. This document is meant to only to convey one experience of this exercise and does in no way describe what may occur in another organization, but similarities should certainly appear.

Data Security/Privacy

Of course, Privacy and Confidentiality must be two of the absolute benchmarks of HIPAA compliance. Total integrity in the storing and transmission of PHI data is a must. Even the agreements between companies must carry what is called HIPAA chain of trust language to insure that the data once passed to a trusted partner is still secure once handed over.

Chain of Trust Agreement

> As the first stage in developing a plan for HIPAA compliance, my organization is in the midst of auditing internal operations. I have been asked to review our current administrative policies and assemble samples of any process maps, policy forms, or procedural outlines of HIPAA mandated administrative procedures that may be helpful to the organization as reference materials. Unfortunately, there isn't a wealth of information about Chain of Trust Partner Agreements. Can you offer some insights?
>
> HIPAA requires the implementation of certain administrative procedures to guard the integrity, confidentiality and availability of data protected under the act. A Chain of Trust Agreement is such a procedure. It is essentially a Non-Disclosure Agreement that governs the transmission of data through an electronic medium. The sender and recipient agree to protect the data electronically transmitted between them.
>
> Chain of Trust Agreements are required when data is processed through a third party. Their purpose is to ensure that a uniform level of security is applied at every "link" in the

> chain where information passes from one party to another. Verification of uniformity at each link is necessary for optimal protection of transmitted data.
>
> It would be extremely onerous, and defeat the purpose of electronic transacting, to require that parties personally confirm use of appropriate security measures before and after each and every transmittal. A Chain of Trust Agreement is a proxy for actual physical confirmation. Therefore, it is very important that the parties to these contracts agree to security mechanisms that:
>
> (1) ensure that all transmissions of data are authorized;
> (2) protect the integrity and confidentiality of patient information; and
> (3) protect business records and data from improper access.
>
> The Agreement should obligate each party to adopt some form of electronic identification (electronic signatures are an example) that unequivocally attributes data transmissions and to agree upon procedures for acknowledging the proper receipt of data. Without these contractual obligations, the parties can't assume any reasonable level of comfort regarding the integrity of transmitted data.
>
> Likewise, without a mechanism to authenticate the origin of transmitted data, it is impossible to establish that the data has not been compromised.
>
> Finally, in order to maintain the integrity of the data passed along this chain, the Agreement should state that the parties will take reasonable measures to maintain equipment, software and other materials that have the potential to negatively impact data and/or the ability to transmit data. Remember the love bug? There are any number of avenues for disabling code or viruses to gain access to an information system. Part of any organization's HIPAA due diligence involves asking software and hardware vendors what procedures they use to protect against these types of intrusions. The potential for data corruption extends beyond the boundaries of two links in a chain. (Fox, Steve Hipaa Advisory with steve Fox)

The use of “shall” and “should” are very important words to follow in the certification process. All shalls must be followed and a certain number of shoulds must be followed in order to obtain a full accreditation from EHNAC. I will not attempt to fully describe the scoring of such. I will only convey the process in which this organization experienced and their possible effects.

The first measure to ensure data security is as follows:
The corporation **shall** have policies to protect against disclosure of personally Identifiable healthcare data. Two examples of this are Company Employee Handbook and Company Non-Disclosure Agreement. These examples were turned over to the decision making body along with all of the evidence which will follow. All of the following criteria were evaluated along with the evidence asked for in each instance. I will attempt to be as brief as possible in each of the following sections. Each of these criteria were requested of the company.

The second measure to ensure data security is as follows:
The corporation **shall** maintain any resource that will ensure a continuing compliance with any data security policies pertaining to secure methods

of transmission and or access of data. Main examples of this again are Company Employee Handbook and Company Non-Disclosure Agreement.

The third measure to ensure data security is as follows:
The corporation **shall** provide to employees any training and or educational resources needed to maintain security compliance. All employees hired will receive prompt company orientation/training that will include an introduction to customer data security, Internet security, computer and email security, internal security, physical security, and an acknowledgement of each employees limited access in and around the company building. Main examples of this are Company Employee Handbook and the new employee training agenda. The corporation has and will conduct numerous on-site training programs concerning many different aspects of HIPAA. Also, the corporation retains the services of HIPAA consultants on a permanent basis. The consultants are used for among other reasons, company wide training courses at all levels in the company. These consultants are among the best in the healthcare industry for sure.

The fourth measure to ensure data security is as follows:
The corporation **shall** support and have plans for utilizing encryption, user authentication, message integrity, non-repudiation in compliance with any and all legislation which requires it. This plan is included in a company security synopsis and made available to the EHNAC auditor when and if on site. 3DES is the only payload encryption allowed in a VPN at this corporation. When AES becomes available, it will be integrated into the security model, as will any improvement in the world of security.

The fifth measure to ensure data security is as follows:
The corporation **shall** use effective controls to protect against all malicious code such as virus, worms, and Trojans. Any and all reasonable industry standard measures will be taken to protect against malicious code, which may affect the internal network and systems. Examples of this will be in the Company Antivirus Protection Plan and also in the Company Employee Handbook.

Technical Performance

Another benchmark of HIPAA compliance is the ability to prove a company's considerable attention to its technical performance. These can be criteria such as expenditures and designs, which will ensure a more secure environment. This category contains 46 shalls and 14 shoulds. Most of these criteria have to do with items such as customer service center related topics. These fall out of the scope of this document and will not be included. The next twenty items/criteria are the included relative criteria, which pertain to Data Security/Privacy. A lengthy discussion will not be attempted (in this report), of each item due to the possibly large amount of information in each of these areas.

The first measure to ensure Technical Performance is as follows:
The corporation **shall** have escalation procedures to follow any internal or customer inquiry to completion. A 24 x 7 365 Data Center is responsible for the tracking of trouble items. This Data Center escalation process will extend to any manager, project manager, engineer, or upper manager until all issues are properly resolved. The manager of the data center will become involved to ensure that the trouble ticket is approached as a team. This Data Center was created and maintained at great expense to the corporation and is a certain asset in regards to any HIPAA related demands. These criteria examples were Data Center Escalation sample trouble tickets and various data scope logs.

The second measure to ensure Technical Performance is as follows:
The corporation **shall** have in place a written disaster recovery plan for the purpose of preventing business interruption. This plan must have procedures for protecting the safety of all employees and the safeguarding of all facilities for the purpose of resuming work.

> The Proposed Security Standard, 45 CFR § 142.308 (a), Administrative procedures to guard data integrity, confidentiality, and availability, requires a "covered entity" (healthcare provider, healthcare organization, healthcare clearinghouse, etc.) to implement "documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data." §§ 142.308 (a)(3) requires that these practices include a **contingency plan**, defined in the proposed regulation as "a routinely updated plan for responding to a system emergency, that includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster."

Customers must be notified according to procedures set forth in this DR plan. Annual DR training exercises must be practiced and written results of these practices must be made available for review. Also annual testing of the capability to resume mission-critical telecom and IT systems must be performed and the written results of such tests must be documented. The company must demonstrate the capability to preserve security while restoration of critical systems is completed. This must be done in a period not to exceed 48 hours.
In response to this item, the company has a 2-part plan to insure high system availability. The first part covers possible catastrophic contingencies and the second part covers the disaster recovery plan itself. These plans were considered even when the construction of the facilities was being carried out. The risk of downtime was an important part of the Data Center design.

The supporting evidence that was needed for this criteria was the Company System Availability and Contingency Plan and also include were items such as maintenance support contracts with vendors such as Telco companies, computer system companies, and contract call centers. Call routing contracts and plans were also required.

The third measure to ensure Technical Performance is as follows:
The corporation **should** have in place a written disaster recovery plan for the purpose of preventing business interruption. This criterion is the same as above except for the time period. This must be done in a period not to exceed 24 hours. Notice that this criteria is a “should” and not a “shall” The supporting evidence for this section is the same except for the time period.

The fourth measure to ensure Technical Performance is as follows:
The corporation **shall** provide audit trails for all data transactions which Involve PHI or the security/privacy of same. All transaction activities are backed up on a daily basis and archived to CD or DVD. These CD/DVD’s are then stored on-site and off-site. They are archived and are immediately retrievable. Although this audit system began in 1995, it is still in use today while utilizing different media for storage. The supporting evidence for this section is CDs with log files. The log from a transaction from 1995 was required and produced in a timely manner. Company far exceeded this requirement.

The fifth measure to ensure Technical Performance is as follows:
The corporation **shall** provide audit trails for two years. The supporting evidence for these criteria is the same as above.

The sixth measure to ensure Technical Performance is as follows:
The corporation **should** provide audit trails for seven years. The supporting evidence for these criteria is the same as above two. Notice that this criterion is a should, while the above is a shall.

The seventh measure to ensure Technical Performance is as follows:
The corporation **shall** provide the capability for a 6-month archive back-up/storage and retrieval system of all critical data. The supporting evidence for these criteria is the same as above three criteria. Also required was a copy of the company’s logging procedures. This corporation made the decision to use what they believe is superior backup software. The software was written by a company named Vertitas. The fact that the software is “certified” for certain platforms can be useful also. Here is a quote from their web site:

VERITAS Disaster Recovery

End-to-End Recovery for Data and Applications

> In the event of a disaster, VERITAS solutions can quickly recover your critical data and applications. VERITAS provides a comprehensive range of software solutions that ensure businesses can continue to operate with minimal interruption. Our disaster recovery solutions support a wide spectrum of operating systems, applications, databases, and hardware platforms and devices to fully protect your heterogeneous IT environments.
> (Veritas website, VERITAS Disaster Recovery)

The eighth measure to ensure Technical Performance is as follows:
The corporation **should** provide the capability or show progress of a 7-year archive back-up/storage and retrieval system of all critical data. The supporting evidence for these criteria is the same as above three criteria. Also required was a copy of the company's logging procedures.

The ninth measure to ensure Technical Performance is as follows:
The corporation **shall** provide the capability to regenerate an EDI transaction from as long ago as ninety days. This must be accomplished in at most two business days. The supporting evidence for these criteria is the same as above three criteria. It's all about the logs.

The tenth measure to ensure Technical Performance is as follows:
Any company seeking a full accreditation and is also connected to the Internet, **shall** have firewall/firewalls in service and configured to protect the systems and other resources on their networks. All company networks and servers are provided by this company. Additionally, all these networks are protected by multiple stateful inspection firewalls. These firewalls are also capable of IPSEC VPNs utilizing 3DES encryption. The web and email servers are all located in a DMZ which are assigned RFC 1918 addresses only. The ports which are open to the public are minimal. All access to this cluster is audited by firewall software and IDS of some undisclosed type. These networks are controlled only by authorized, trained personnel through inside access only. No outside (Internet) management is allowed. The use of port scanning software is authorized inside and out of the dmz in order to ascertain any open port or ports that may have been inadvertently opened. All firewall logs are dumped and saved on a regularly scheduled basis. The company maintains contracts with firewall vendor for upgrades, patches and emergency work. All of the firewalls are built by company personnel along with the involvement of a vendor. This process helps retain total control of critical system capabilities and leaves less possibility for holes or backdoors.

The supporting evidence for these criteria was firewall end user licenses, actual license string printouts and finally, evidence of any subscription agreements. A network diagram was also provided.

The eleventh measure to ensure Technical Performance is as follows:

The corporation **shall** utilize strong encryption for any PHI that may traverse the Internet or any other known insecure network. The preferred method of data transfer is over permanent private circuits. When permanent private circuits cannot be used then a “firewall to firewall” (IPSEC) VPN will be used or SSL version 3.0 or later. All data transfer platforms are members of their own dmz as well. All dmzs are separated by firewalls.
The supporting evidence for above was the Certificates from a well-known CA. A network diagram was also provided for this section as well.

The twelfth measure to ensure Technical Performance is as follows:
The corporation **shall** utilize a software/hardware product to control/monitor or block any or all attempted intrusions or attacks from the Internet or from possible inside intruders. This will also include alarms, logs and reporting to the proper personnel. The corporation achieves this by the use of an OPSEC certified Internet security platform product called Entercept. This product is installed on multiple systems and is monitored 24x7 365. Supporting evidence for this criteria will be logs from the product and a deployment process document. License agreements for the IDS products were also provided to the certifying board. The following quote is from Entercept Security Technology.

> ***Intrusion Prevention Solutions for the Healthcare Industry***
>
> The healthcare and pharmaceutical industries have seen dramatic changes in the way they conduct business as the Internet has evolved. Electronic transfer of information has streamlined processes that were paper-based only a few years ago.
>
> **Healthcare Industry**
> Medical research and records are now accessible easily and shared electronically between healthcare organizations and patients. In addition, patients are now empowered to view and manage their own health records online. While electronic delivery is more efficient and cost-effective, the data that is being transferred over multiple networks and that resides on back-end servers are vulnerable targets for malicious attacks.
>
> **Pharmaceutical Industry**
> Pharmaceutical companies are now able to communicate electronically with regulatory agencies such as the Food and Drug Administration, consumers for medical prescriptions and clinical trial data records. As information is transferred and accessed online, pharmaceutical companies are streamlining their business processes with lower operational expenses. However this makes the medical/drug records vulnerable for malicious attacks as well. (Entecept IDS and Healthcare)

Both of these areas, Healthcare Industry and Pharmaceutical Industry, apply to this corporation.

The thirteenth measure to ensure Technical Performance is as follows:
The corporation **shall** utilize a software/hardware product to control all bandwidth needs on all firewalls that pass PHI data. This company uses a plug-in product that cab be installed on all firewalls. The name of this product will remain undisclosed in order to de-identify the firewall model or manufacturer.
The supporting evidence that was used for this section was logs of dmz inbound/outbound data transfer rates.

The fourteenth measure to ensure Technical Performance is as follows:
The corporation **shall** provide any documented procedures that describe responses to apparent pre-intrusions, intrusions or possible post intrusions from the Internet. Company must have documented procedures for restoring compromised systems within 4 hours of a proven attack. Supporting evidence for this section was the company deployment manual for DMZ systems.

The fifteenth measure to ensure Technical Performance is as follows:
The corporation **shall** on a scheduled basis perform threat and vulnerability tests. (pentest) The companies Disaster Recovery Plan addresses any company web cluster or dmz systems recovery. The supporting evidence again is the DRP.

The sixteenth measure to ensure Technical Performance is as follows:
The corporation **should** be able to begin to respond to any intrusion within one hour of any significant attack alarm. Company should possess documented procedures for the proper response to intrusion within a two-hour period of time. The supporting evidence for this criteria was same as fourteenth criteria. Deployment manual for the DMZ systems.

The seventeenth measure to ensure Technical Performance is as follows:
The corporation **shall** thoroughly document all web security configurations to help protect cluster from intrusions. The company cluster is in a protected dmz with all of the protections which are documented in some of the above criteria. These documents were provided in above sections.

The eighteenth measure to ensure Technical Performance is as follows:
The corporation **shall** have documented procedures to check security of web cluster from outside locations. This is intended to ensure that potential weaknesses are minimal and that the web server O/S and application configurations are up to date.
Evidence of this was provided in a Web Security Assessment procedure document.

The nineteenth measure to ensure Technical Performance is as follows:
The corporation **shall** not operate any FTP server/servers that are configured in a manner to allow files to pass without port forwarding through a firewall.
Some FTP servers are filtered on IP addresses and some are open to any source address. All FTP servers are for FTP only. No other ports are allowed

from any other network once they are in production. Any port that will be opened for a temporary period will be done so only when that particular server is taken out of production. All traffic to and from these FTP servers are logged in several different places, in NIDS, HIDS and firewalls. Logging will also be done at the service/daemon level on the server.
Supporting evidence fir this section was present in the unnamed company product customer agreement.

The twentieth measure to ensure Technical Performance is as follows:
The corporation **shall** ensure that any databases that are internal not be allowed to be modified directly through a web site. All modifications to databases will be made by application only to a local database and then after an integrity check the modification will be synchronized to any internal database. All databases are located on protected networks which utilize OS, database engine, and finally application security models for the transfer of PHI data from system to system.
Supporting evidence for this section was a narrative and the network diagram.

Business Practices
(There were no security/network related criteria in this section)

Resources/Protection of Data and Equipment

The first measure to ensure Protection of Data and Equipment is as follows:
The corporation **shall** have physical security that is equal to or greater than needed to ensure the confidentiality and integrity of all data and equipment pertaining to the transfer, storage, or viewing of PHI data. This criteria has much to do with the actual design and usage of the building itself. This especially pertains to the DataCenter and all areas for testing, development, and the implementation of critical systems that will be or have been used. Each floor must be carefully planned for access and logging of access. In our case, proximity cards are used along with some keyed doors that require both. There are operators present 24x7 365. No unauthorized person should be able to access any system in the datacenter without the operators knowing who and what. Alarms are sent to the datacenter when an authorized person enters a telco closet or switch room at any time. All access is limited to one team that the operators also belong to. In other words, any time there is an entry to any area containing equipment described in this section, everyone is aware of this entry. Every entry door including the elevator after hours has proximity detectors. ONLY Persons in the group that maintains this equipment and data have access to it through configured entry points. This even pertains to the CEO or any person in the corporation. Entrance will be granted on basis of management decision.

Supporting evidence for this section was a table of time on/time off security schedules for all major sub systems including card readers, fire detection, alarm systems, cameras, etc… Of course a visit to the physical location was scheduled and performed. This was a visit by a board member of the certifying board.

The second measure to ensure Protection of Data and Equipment is as follows: The corporation **shall** ensure that all PHI data is protected by password policies which hold that passwords are changed at period intervals and also when personnel change positions within the company. This includes a section of the policy that ensures that when an employee of any type terminates, or a breach is identified, policies are in place to remove or modify that account to remove any danger of unauthorized access.
Supporting evidence for this was printouts of system password policies and also copies of written policies pertaining to the area of password management.

The third measure to ensure Protection of Data and Equipment is as follows: The corporation **should** maintain policies and procedures that hold to a system of authorization which will limit internal and external sources from accessing tables, databases, or any transmitted data. This system of authorization will adhere to a multi-layered approach. This corporation fully adheres to the proposed HIPAA rule and the HCFA Internet Security Policy. Following is a quote from the HCFA policy. This policy is followed for the purposes of three areas of security. Authenticaton, identification, and encryption. Notice that this criteria is a should and not a shall. This was taken from Image Management Systems and Support Corp. They took it from Office of Information Services, HCFA Security and Standards Group Division of HCFA Enterprise Standards -Internet

> This Guide establishes the fundamental rules and systems security requirements for the use of the Internet to transmit HCFA Privacy Act-protected and other sensitive HCFA information collected, maintained, and disseminated by HCFA, its contractors, and agents.
>
> It is permissible to use the Internet for transmission of HCFA Privacy Act-protected and/or other sensitive HCFA information, as long as an acceptable method of encryption is utilized to provide for confidentiality and integrity of this data, and that authentication or identification procedures are employed to assure that both the sender and recipient of the data are known to each other and are authorized to receive and decrypt such information. Detailed guidance is provided below in item 7. (HCFA Internet Security Policy", HCFA Privacy Act)

A narrative was provided as supporting evidence of this criteria.

The fourth measure to ensure Protection of Data and Equipment is as follows:

The corporation **should** maintain an ongoing accurate log of any changes made to table, files or databases. This company uses a hard copy update and access log to perform all database and file updates. Copies of these logs are on file in the data center. Also products such as SourceSafe are used to log many changes to code files and data files. All logs are archived and available for review by authorized personnel. Notice this was a should.

The fifth measure to ensure Protection of Data and Equipment is as follows:
The corporation **shall** all proper hardware, software, and any physical resource needed to carry out the company's stated mission.
The company provided any certificates of compliance from vendors, licenses and Inventories of all equipment and software. This was easy since the company has been doing this from the start.

The sixth measure to ensure Protection of Data and Equipment is as follows:
The corporation **should** log all company/operator system access violations.
This criteria was supported by update logs of many types. Notice also that this was a should and not a shall.

The seventh measure to ensure Protection of Data and Equipment is as follows:
The corporation **shall** possess a formal expansion plan. This plan will include any growth which may affect Network or Security areas. This plan will be reviewed on a regular basis.
Supported evidence for this criteria was a company narrative concerning the Building Lease Agreement, which is classified proprietary.

The eighth measure to ensure Protection of Data and Equipment is as follows:
The corporation **shall** employ a sufficient number of qualified personnel to fulfill stated company mission.
Supported evidence for this criteria was a company narrative concerning the monitoring of expanding headcount and efficiency of each position.

The ninth measure to ensure Protection of Data and Equipment is as follows:
The corporation **shall** provide training and resources for the knowledge and enrichment of each employee. Especially when their area has access to PHI related data. Supported evidence for these criteria was the company schedule of product training, new employee training (which includes training on the protection of PHI data) and formal HIPAA training from the industries most knowledgeable HIPAA experts. The company also provides departmental level training for employees handling or accessing PHI. This training should include at least a yearly session concerning privacy, confidentiality, and security. Supported evidence for these criteria was a formal schedule of upcoming training programs.

The tenth measure to ensure Protection of Data and Equipment is as follows:
The corporation **shall** create and publish to all employees an explicit policy, which covers the privacy and confidentiality and the protection against

unauthorized disclosure of any de-identified PHI of any type. This includes all real-time, production, test, or development data.
Supported evidence for these criteria was the company employee handbook and all policies that are referenced therein.

All of the above evidence from each of the four sections described was turned over to representatives of the EHNAC organization. After its review and after a period of time, a determination was made as to the compliance of the corporation. In some states, a corporation must obtain this or another “certification” like it in order to do business with that state. These certifications can also be helpful in soothing the paranoia that potential trading partners may have. The law concerning PHI can be extremely frightening, Following is a quote concerning the Privacy mandate.

> "You need to have a signed agreement with each of your business partners," says Stephen Brown, an attorney with Bogatin Law Firm of Memphis, Tenn., which has been closely following the HIPAA saga. "The agreement should stipulate that business associates won't disclose protected medical information and that they will make appropriate records available to the Department of Health and Human Services, if needed, to prove they took protective measures."
>
> "It's fairly onerous," says Richard Peterson, director in Computer Sciences' global health solutions division. "You have to get consent from the patient in order to share data with business associates as well as other healthcare providers and pharmaceutical organizations."
>
> In addition, each HIPAA-covered healthcare organization will have to document privacy practices and security policies - and this, say lawyers, will aid greatly should an organization have to defend itself against charges of defying HIPAA. (Messmer, Ellen Network World, 02/12/01)

This process was also a healthy exercise in self-evaluation, which proves to be extremely helpful from a security prospective. It can prove to have a “bringing it all together” effect on what already exists, or the process can be used for implementation as well. Either way, it can be a tough experience, but necessary. Certification can be useful in any area right? Of course.

References

1. “Healthcare Network Accreditation.” EHNAC website Default Page. 6/10/02 url: http://www.ehnac.org/Accreditation/Default.html (4/14/03)
2. What is EHNAC Healthcare Network Accreditation? Frequently Asked Questions for the Electronic Healthcare Transaction Industry url: http://www.ehnac.org/Accreditation/Overview.html (4/14/03)
3. Fox,Steve. “Chain of Trust Agreements” Hipaa Advisory with steve Fox url:http://www.hipaadvisory.com/action/LegalQA/advisor/HIPAAdvisor5.htm (4/15/03)
4. “End-to-End Recovery for Data and Applications”. VERITAS Disaster Recovery (2003) url:http://www.veritas.com/products/category/ProductFamily.jhtml?baseId=2001 (4/17/03)
5. Hughes,Kristen K. “HIPAA and Disaster Recovery” 6/10/02 url:http://www.reillycomm.com/it_archive/it_ip0102_HIPAA.htm (4/16/03)
6.” Entecept IDS and Healthcare” (2003) url:http://www.entercept.com/industry/healthcare/
7.” HCFA Internet Security Policy” HCFA Privacy Act (Extension of Privacy Act of 1974) url:http://www.imss.net/hcfa-policy.htm
8. (Messmer, Ellen. Network World, 02/12/01)